UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,578	03/27/2007	Dennis Vance Pollutro	2006579-2113 (CTX-624)	8867

69665 7590 06/24/2010

CHOATE, HALL & STEWART / CITRIX SYSTEMS, INC.
TWO INTERNATIONAL PLACE
BOSTON, MA 02110

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
06/24/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTDOCKET@CHOATE.COM
jhess@choate.com
lbradley@choate.com

Office Action Summary	Application No.	Applicant(s)	
	10/583,578	POLLUTRO ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/19/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to original filing June 19, 2006. Claims 1-21 are pending.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Currently, claim 21 is drawn to a "computer readable carrier" including a computer product. The term "carrier" however suggests the inclusion of a transitory signal for which the office considers to be non-statutory subject matter. As such the applicant is advised to do the following:

a. Replace "computer readable carrier" with "computer readable recording medium"

b. Remove the recitation of radio frequency carrier wave, audio frequency carrier wave, etc.) from [0036] and [0046].

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 14, 15, and 21 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 15, 18, 22, and 32 of (U.S. Patent No. 7,644,434 Pollutro(2)) in view of Williams (US Patent Publication No. 2003/0005118). Pollutro (2) discloses: modifying a message to be transmitted during a session between a client and a server system to include a session identification flag and a session identifier corresponding to an originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system; transmitting the message between the client and the server system; checking the transmitted message for the session identification flag;. Pollutro(2) does not expressly teach reading the session identifier of the transmitted

message to determine the originator of the message.. However, at the time of applicant's original filing, the feature of using a session identifier to determine the originator of a message was well known in the art and would have been an obvious modification of Pollutro (2) as discloses by Williams. Williams discloses using a session identifier to determine the originator of a message [par. 64]. Therefore given Pollutro(2)'s use of session identifiers in communication, a person of ordinary skill in the art would recognize the advantage of modifying Pollutor(2) to enhance network access control with the well known feature of using a session id to identify a user as disclosed by Williams.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Williams (US Patent Publication No. 2003/0005118).

3. As to claim 1, Williams teaches a method of Identifying the originator of a message transmitted between a client and a server system [par. 62], said method comprising the steps of:

modifying (e.g., inserting) a message to be transmitted during a session between a client and a server system to include a session identification flag and a session identifier corresponding to an originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system (i.e., ...teaches the server may identify the client based upon the presented token [abstract]. ...teaches service token, which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the established session. ...further teaches inserting session id into the token [par. 62]);

transmitting the message between the client and the server system (i.e., ..teaches the client also sends a single-use service token [par. 63]);

checking the transmitted message for the session identification flag [408, fig. 4a];

and reading (e.g., using) the session identifier of the transmitted message to determine the originator of the message (i.e., ..teaches the protected server uses the session ID in the service token to match the previously established session context with the client [par. 64]).

4. As to claim 2, William teaches a method where the step of modifying the message comprises the step of re-computing (e.g., generate) a control portion (e.g., data field) of the message to reflect the inclusion of the session identification flag and the session Identifier (e.g., session information) (i.e., ...teaches a session ID can be issued by the protected server and inserted in the service token; the session information is a session key contained in the data field of the cookie. ...returns a newly generated service response message which comprises service token containing session information [par. 62]).

5. As to claim 3, William teaches a method further comprising the steps of: removing the session identification flag and the session identifier from the transmitted message (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the previously established data [par. 64] ...note the William states that the session information is used thereby suggesting that the data was removed from the packet);

and re-computing (e.g., refreshed) the control portion (e.g., service token) of the message to reflect the removal of the session identification flag and the session identifier (i.e., ...teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token a single use token suggesting that the session has been established [par. 66]).

6. As to claim 4, William teaches a method where the step of modifying the message (e.g., token) comprises appending the session identification flag and the session identifier at an end of the message (i.e., ...teaches session information is included in the token (e.g., packet/message) [par. 62])

7. As to claim 5, William teaches a method where the step of modifying the message further comprises at least one of changing the session identifier for each communication or changing the session identifier at a predetermined interval (i.e., ..teaches a single-use service token can be asserted only once by its owning entity, i.e. the entity with which the service token is associated. After a single-use service token has been used, it cannot be re-used without being refreshed or updated by its issuing entity so that it may be used again [par. 66]).

8. As to claim 6, William teaches a method of identifying the originator of a communication packet (i.e., ...teaches the server may identify the client based upon the presented token [abstract]);

transmitted between a client and a server in a client/server system (i.e., teaches the client also sends a single-use service token [par. 63]), said method :comprising the steps of: appending a session identifier and a security tag (i.e., data field) to the communication packet (i.e., cookie) (i.e., ...teaches session information is a session key contained in the data field of the cookie [par. 62]), the session identifier uniquely

identifying the client in the client/server system (i.e., ... teaches server may identify the client based upon the presented token. ..further teaches the token comprises a session identifier [abstract];

authenticating (e.g., matched the session identifier using the security tag (e.g., session context) (i.e., ...teaches the session ID is subsequently matched to the client's session context when received by the protected server [par. 62]);

if the appended session identifier is authenticated determining the originator of the transmitted communication packet based on the appended session identifier (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]).

9. As to claim 7, William teaches a method further comprising the step of: establishing a common security tag in the client and server (i.e., ...teaches establishing a session id (e.g., security tag) between server and client [par. 62]),

wherein the step of appending the session identifier includes appending the common security tag to the communication packet to be transmitted between the client and the server such 5 that a presence of the common security tag in the transmitted communication packet 6 indicates that the session identifier is authenticated (i.e., teaches inserting (i.e., appending) session id [par. 62]).

10. As to claim 8, William teaches a method further comprising the steps of: if the appended session identifier in the transmitted communication packet is authenticated, processing the transmitted communication packet according to predetermined rules for transmitted communication packets with authenticated session identifiers (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]);

and if the appended session identifier in the transmitted communication packet is not authenticated, processing the transmitted communication packet according to predetermined rules for transmitted communication packets without authenticated session identifiers (i.e., ...teaches asserting a stale or invalid token would result in a failed operation and optionally other security measures [par. 66]).

11. As to claim 9, William teaches a method where the step of appending (e.g., inserting) the session identifier and the common security tag to the communication packet {par. 62] comprises the step of re-computing (e.g., generating) a control portion of the communication packet to be transmitted to reflect the inclusion of the common security tag and the session identifier (e.g., session information) (i.e., ...teaches a session ID can be issued by the protected server and inserted in the service token; the session information is a session key contained in the data field of the cookie. ...returns a newly generated service response message which comprises service token containing session information [par. 62]), the method further comprising the steps of:

removing the session identification flag and the session identifier from the transmitted message (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the previously established data [par. 64] …note the William states that the session information is used thereby suggesting that the data was removed from the packet);

and re-computing (e.g., refreshed) the control portion (e.g., service token) of the message to reflect the removal of the session identification flag and the session identifier (i.e., …teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token a single use token suggesting that the session has been established [par. 66]).

12. As to claim 10, William teaches a method further comprising the steps of: encrypting the communication packet to be transmitted after the step (i.e., teaches any information within a token may be encrypted to hide the information so as to limit the risk that it might be misappropriated [par. 50]);

appending (i.e., inserting) the session identifier and the common security tag [par. 62];

and decrypting the transmitted communication packet prior to the steps of determining the originator of the transmitted communication packet (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]),

removing the common security tag and the session identifier (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the previously established data [par. 64] ...note the William states that the session information is used thereby suggesting that the data was removed from the packet),

and re-computing (e.g., refresh) the control portion of the transmitted communication packet (i.e., ...teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token a single use token suggesting that the session has been established [par. 66]).

13. As to claim 11, Williams teaches a method further comprising the steps of: encrypting the communication packet to be transmitted prior to the step of appending the session identifier and the common security tag (i.e., teaches any information within a token may be encrypted to hide the information so as to limit the risk that it might be misappropriated [par. 50]); and decrypting the transmitted communication packet after the step of re- computing the control portion of the transmitted communication packet (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]).

14. As to claim 12, Williams teaches a method further comprising the step of: setting a length of the common security tag (i.e., session information) greater than a

predetermined length to reduce or substantially eliminate falsely authenticated session identifiers (i.e., teaches inserting the session information into a data field [par. 62]).

15. As to claim 13, Williams teaches a method according where the length of the security tag is set to a length in the range of about 8 to 64 bits long [par. 62].

16. As to claim 14, William teaches a method of identifying an originator of all communication packets transmitted between a client and a server system using an application program [fig. 2b], the originator having an actual network address (i.e., ...teaches client machine's IP address [par. 57]); said method comprising the steps of:

Modifying (i.e., inserting) each of the communication packets to be transmitted between a client and a sever system to include information (e.g., session id) identifying the originator of a respective communication packet without regard for the application program being used or an apparent network address that is a network address that replaces the actual network address of the originator during transmission of a respective communication packet (i.e., ...teaches the server may identify the client based upon the presented token [abstract]. ...teaches service token, which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the established session. ...further teaches inserting session id into the token [par. 62]);

transmitting each modified communication packet between the client and the sever system (i.e., teaches the client also sends a single-use service token [par. 63]);

and determining the originator of each transmitted communication packet based on the information identifying the originator therein (i.e., ...teaches the server may identify the client based upon the presented token [abstract] ..further teaches the token contains a session id [abstract]) .

17. As to claim 15, William teaches a computer system for identifying the originator of a message [abstract], comprising: a server [fig. 2B]; and a client operationally connected to the server [fig. 2B], the client and server being configured to transmit one or more messages there between during a session [fig. 2B], each of the messages to be transmitted being modified by one of the client or the server to include a session identification flag and a session identifier (i.e., ...teaches the server may identify the client based upon the presented token [abstract]. ...teaches service token, which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the established session. ...further teaches inserting session information into the token [par. 62]);

the client and server being further configured such that the modified message is transmitted (e.g., send) to the remaining one of the client and the server (i.e., teaches the client also sends a single-use service token [par. 63]);

the session identification flag of the transmitted message is checked by the remaining one of the client and the server to validate the session identifier (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]);

and if the session identifier is validated, the session identifier of the transmitted message is read to determine the originator of the transmitted message (i.e., teaches the CDC authenticates the client or user by processing the authentication data to determine whether or not the client or the user that is asserting itself has properly established its identity [par. 69]),

the session identifier corresponding to an originator of a session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system (i.e., ..teaches the session id is used to identify the client [abstract]).

18. As to claim 16, William teaches a computer system further comprising a network gateway disposed operationally between the client and server and providing access to the server such that the server is remotely accessible by the client [fig. 2B].

19. As to claim 17, William teaches a computer system further comprising: an encrypting unit disposed on one side of the network gateway to encrypt the message to be transmitted (i.e., teaches any information within a token may be encrypted to hide the information so as to limit the risk that it might be misappropriated [par. 50]).

20. As to claim 18, William teaches a computer system further comprising: a decrypting unit disposed on another side of the network gateway to decrypt the transmitted message (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]).

21. As to claim 19, William teaches a computer system where the message is processed sequentially such that either the message to be transmitted is encrypted by the encrypting unit and then modified and the transmitted message is read and then decrypted by the decrypting unit or the message to be transmitted is modified and then encrypted by the encrypting unit and the transmitted message is decrypted by the decrypting unit and then read (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]).

22. As to claim 20, William teaches a computer system where the network gateway includes a database to validate the session identifier by checking a user identifier (i.e.,

teaches the CDC authenticates the client or user by processing the authentication data to determine whether or not the client or the user that is asserting itself has properly established its identity [par. 69]), if the session identifier is not valid, the computer system forces the user to log in prior to accessing the server and if the session identifier is valid, the computer system retrieves an associated user identifier (i.e., ...teaches asserting a stale or invalid token would result in a failed operation and optionally other security measures [par. 66]) and the server processes the transmitted message (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]).

23. As to claim 21, Williams teaches computer readable carrier including computer program instructions which cause a computer system including at least a client and a server to implement a method of identifying the originator of a message transmitted between the client and the server (i.e., ..teaches establishing the identity of a client [abstract], said method comprising the steps of:

modifying (e.g., insert) a message to be transmitted during a session between the client and the server to include a session identification flag and a session identifier, the session identifier being assigned corresponding to the originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system (i.e., ...teaches the server may identify the client based upon the presented token [abstract]. ...teaches service token,

which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the established session. ...further teaches inserting session information into the token [par. 62]);

re-computing (e.g., generating) a control portion of the message to reflect the inclusion of the session identification flag and the session identifier (e.g., session information) (i.e., ...teaches a session ID can be issued by the protected server and inserted in the service token; the session information is a session key contained in the data field of the cookie. ...returns a newly generated service response message which comprises service token containing session information [par. 62]);

transmitting the message between the client and the server (i.e., teaches the client also sends a single-use service token [par. 63]);

checking the transmitted message for the session identification flag [408, fig. 4a];

reading (e.g., using) the session identifier of the transmitted message to determine the originator of the message (i.e., ..teaches the protected server uses the session ID in the service token to match the previously established session context with the client [par. 64]);

removing the session identification flag and the session identifier from the transmitted message (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the

previously established data [par. 64] …note the William states that the session information is used thereby suggesting that the data was removed from the packet);

and re-computing (e.g., refreshed) the control portion (e.g., service token) of the message to reflect the removal of the session identification flag and the session identifier (i.e., …teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token a single use token suggesting that the session has been established [par. 66]).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431